fm

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/541,667	03/31/2000	Carl M. Ellison	042390.P8629	3630

7590 03/03/2004

Thinh V Nguyen
Blakely Sokoloff Taylor & Zafman LLP
12400 Wilshire Boulevard
7th Floor
Los Angelos, CA 90025

EXAMINER	
TRAN, TONGOC	
ART UNIT	**PAPER NUMBER**
2134	15

DATE MAILED: 03/03/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

fm

Office Action Summary	**Application No.** 09/541,667	**Applicant(s)** ELLISON ET AL.	
	Examiner Tongoc Tran	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 January 2004*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-80* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-80* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 13/14.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This office action is in response to applicants' amendment filed on 1/14/2004. Claims 17-19, 37-39, 57-59 and 77-79. Claims 1-80 are pending.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 1/28/2004 has been considered by the examiner

Response to Arguments

3. Rejection under 35 U.S.C. § 102

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "one processor with two modes of operations and an isolated execution mode includes configuration of isolated execution, definition of an isolated area, definition of isolated instruction...") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns,* 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Applicants also contend that Davis does not teach a communication storage and that there is no remote attestation. The examiner respectfully disagrees. Davis discloses a communication storage and a remote attestation (see col. 3, lines 15-30, stored within second electronic system and certification authority)..

Rejection under 35 U.S.C. § 103

Applicants contend that there is no motivation to combine Davis [004], Ermolovich and Davis [981] because none of them addresses the problem of isolated execution mode. The examiner respectfully disagrees. Davis [004] clearly discloses a processor with an isolated execution mode (see Davis [004], col. 4, lines 38-47, processing unit performs computations on the data set internally within a secure environment (i.e. an environment with minimal vulnerability to a physical or algorithmic attack) col. 6, lines 13-21, host processor having the functionality in the form of protected execution capability). Applicants contend that there is no motivation to combine Davis with Ermolovich because Ermolovich does not teach a "configuration storage" for an isolated execution mode. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., configure storage) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns,* 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Furthermore, applicants contend that Davis [986] merely discloses a BIOS upgrade, not a configuration of device to exchange security information with a processor having a normal and isolated execution modes. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art.

See *In re Fine,* 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones,* 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, [Davis 986] discloses the features of configuration which is old and well known in the computer art by storing product information and version for producer configuration and/or product upgrade. Combining it with Davis [004]'s teaching of "at least one processors operating in one of a normal execution mode and an isolated execution mode" would have been obvious because otherwise nothing will work.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless --
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351 (a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-5, 21-25, 41-45 and 61-65 are rejected under 35 U.S.C. 102(e) as being anticipated by Davis (U.S. Patent No. 6,357,004).

The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

In respect to claim 61, Davis discloses a system comprising:

"at least one processor operating in ,a secure environment, the at least one processor having one of a normal execution mode and an isolated execution mode (see Fig. 2, items 135 and 105, col. 3, lines 55-63);

a memory coupled to the at least *one* processor, the memory having an isolated memory area accessible to the at least one, processor in the isolated execution mode (see col. 3A, item 205 and 210, col. 4, linen 29-41); and

a chipset couple to the at least one processor and the memory, the chipset having a circuit (see Fig. 2, col. 3, lines 55-63), the circuit comprising:

an interface to map a device via a bus to an address space of the chipset in the secure environment (see Fig. 2 and Fig. 3A, col. 3, lines 55-63 and col. 4, lines 38-41), and

a communication storage corresponding to the address space to allow the device to exchange security information with the at least one processor in the isolated execution mode in a remote attestation" (see Fig. 2 and 3A, col. 3, lines 15-30 line 55and col. 4, line 2 and lines 48-58).

In respect to claim 62, Davis further discloses, "wherein the security information includes at least one of a static public key and a static key certificate" (see col. 3, lines 15-30).

In respect to claim 63, Davis further discloses, "wherein the interface comprisesa decoder to decode the address space onto the bus so that an access to the chipset is passed to the device (see col. 4, lines 37-47, decompression).

In respect to claim 64, Davis further discloses, "wherein the device accesses a chipset storage via the address space" (see Fig. 2 and col. 3, line 55-col. 4, line 2). In respect to claim 65, Davis further discloses, "wherein the communication storage comprises: a configuration storage to store device configuration information (see col. 7, lines 5-12).

Claims 1-5 are apparatus claims that are substantially equivalent to the system claims 61-67 and therefore are rejected by a similar rationale.

Claims 21-25 are method claims that are substantially equivalent to the system claims 61-67 and therefore are rejected by a similar rationale.

Claims 41-45 are computer readable medium claims that are substantially equivalent to the system claims 61-67 and therefore are rejected by a similar rationale.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 6-7, 9-19, 26-27, 29-39, 46-47, 49-59, 66-67 and 69-79 are rejected under 35 U.S.C. 103(x) as being unpatentable over Davis (U.S. Patent No. 6,357,004) in view of Ermolovich (U.S. Patent No. 4,319,233).

In respect to claim 66, Davis discloses the communication storage as applied to claim 65 but does not explicitly discloses said storage comprises:

"a status register to store device status of the device;

a command register to store a device command for a command interface set; and

an input/output block(IOB) to store input and output data corresponding to the command".

However, Ermolovich discloses a status register to store device status (see col. 85, lines 37-45), a command register to store a device command (see col. 12, lines 2-6) and an input/output block to store input and output data (see col. 71, lines 40-64). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Davis' system of ensuring integrity throughout post processing with the teaching of Ermolovich's communication device with data processing system by including the status register, the command register and the input/output block taught by Ermolovich to prevent data from being lost or corrupted during data transfers between a data processing system and an external device (see Ermolovich et al. abstract and col. 3, lines 26-50).

In respect to claim 67, Davis and Erimolovich disclose the system of claim 66. Davis further discloses, "wherein the configuration storage comprises:

a public key storage to store the static public key; a key certificate storage to store the static key certificate (see col. 4, lines 48-58); and

an interface set storage to store an interface set identifier, the interface set identifier identifying a command interface set supported by the device (see col. 4, lines 4, lines 48-58).

In respect to claim 69, Davis and Ermolovich disclose the system of 67. Ermolovich further discloses, "wherein the command interface set is an initialization set, the initialization set supporting a reset command and a connect command" (see col. 54, lines 20-28).

In respect to claim 70, Davis and Errnolovich disclose a system of claim 67. Davis further discloses "wherein the command interface set is an attestation set, the attestation set performing at least one of a public key enumeration, a key certificate enumeration, and signing operation" (see col. 4, lines 48-53).

In respect to claim 71, Davis and En-nolovich disclose the system of claim 70. Ermolovich further disclose, "wherein the status register comprises:

a connection field to provide a connection status to indicate that the device is responsible to the connect command (see col. 9, lines 7-17); and

an estimate field to provide an estimate of processing time for an operation specified in the command" (see col. 16, lines 1-14).

In respect to claim 72, Davis and Erimolovich disclose the system of claim 71. Ermolovich further discloses "wherein the status register further comprises:

a self-test field to indicate status of a self test in response to the reset command" (see col. 86, lines 4-21).

In respect to claim 73, Davis and Erimolovich disclose the system of claim 70. Davis further discloses, "wherein the public: key enumeration enumerates an additional public key than the static public key" (see col. 4, lines 29-36 and lines 48-53).

In respect to claim 74, Davis and Ermolovich disclose the system of claim 70. Davis further discloses, "wherein the key certificate enumeration enumerates an additional key certificate other than the static key certificate" (see col. 4, lines 29-36 and lines 48-53).

In respect to claim 75, Davis and Ermolovich disclose the system of claim 70. Davis further discloses, "wherein the sign operation generates a signature to attest validity of the secure environment using a private key provided by the chipset" (see col. 2, lines 55-65).

In respect to claim 76, Davis and Ermolovich disclose the system of claim 75. Davis further discloses, "wherein the signature corresponds to signing a chipset parameter" (see col. 2, lines 55-65).

In respect to claim 77, Davis and Ermolovich disclose the system of clam 76. Davis further discloses, "wherein the chipset parameter is a software hash" (see col. 2, lines 41-54).

In respect to claim 78, Davis and Ermolovich disclose the system of claim 77. Davis further discloses wherein the processor nub loader hash arid the chipset hash log are stored in the chipset storage (see col. 6, line 57-col. 7, line 30).

In respect to claim 79, Davis and Ermolovich disclose the system of claim 78. Davis further discloses wherein the software hash and the nonce are provided by a processor nub (see col. 6, line 57-col. 7, line 30).

Claims 6-7 and 9-19 are apparatus claims that are substantially equivalent to the system claims 66-67 and 69-77 and therefore are rejected by a similar rationale.

Claims 26-27 and 29-39 are method claims that are substantially equivalent to the system claims 66-67 and 69-77 and therefore are rejected by a similar rationale.

Claims 46-47 and 49-59 are computer readable medium claims that are substantially equivalent to the system claims 66-67 and 69-77 and therefore are rejected by a similar rationale.

8. Claim 8, 28, 48 and 68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis (U.S. Patent No. (3,357,004, hereinafter Davis [`004]) and Ermolovich (U.S. Patent No. 4,319,323) as applied to claim 67 above, and further in view of Davis (U.S. Patent No 5;844,986 hereinafter Davis [`986]).

In respect to claim 68, Davis [`004] and Ermolovich disclose the configuration storage as applied to claim 67. Davis [`004] and Ermolovich do not explicitly disclose, "wherein the configuration storage further comprises:

A manufacturer identifier storage to store a manufacturer identifier; and

A revision storage to store a revision identifier. However, Davis [`986] discloses manufacture identifier storage (see col. 3, lines 37-45, software manufacture (BIO vendor), BIO code) and a revision storage to store revision identifier (see col. 4, lines 7-

13, revision date). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate Davis [`004] and Ermolovich's teachings with Davis' [`986] teaching of storing a manufacturer identifier and revision identifier for the purpose identifying product manufacture and product version information in order to determine product compatibility and perform product upgrade.

Claim 8 is an apparatus claim that is substantially equivalent to the system claim 68 and therefore is rejected by a similar rationale.

Claim 28 is a method claim that is substantially equivalent to the system claim 68 and therefore is rejected by a similar rationale.

Claim 48 is a computer readable medium claim and is substantially equivalent to the system claim 68 and therefore is rejected by a similar rationale.

Conclusion

9. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from.the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action. 10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (703) 3057690. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http-//pair-direct.uspto.gov. Should you have questions on access to the **Private PAIR** system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran
Art Unit: 2134

TT
February 25, 2004

Matthew B. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137